Amendments to the Specification:

Please replace the paragraph extending from page 1, line 36 to page 2, line 13, with the following amended paragraph:

In accordance with one embodiment of the present invention, a method includes emulating a SMTP client application including generating at least one SMTP client application dirty page. The method further includes emulating an executable application sent from the SMTP client application including generating at least one executable application dirty page. The method further includes determining whether the at least one SMTP client application dirty page is a match of the at least one executable application dirty page. If a determination is made that the at least one SMTP client application dirty page is a match ~~and~~ of the at least one executable application dirty page, a determination is made that the SMTP client application is polymorphic malicious code that is attempting to send itself and protective action is taken.

Please replace the paragraph extending from page 3, line 19 to line 30, with the following amended paragraph:

In accordance with one embodiment, referring now to FIG. 2, a method includes establishing a SMTP proxy in an establish SMTP proxy operation 204, defining an application that forms a connection with the SMTP proxy as a SMTP client application in a SMTP client application connects to proxy operation 206, emulating the SMTP client application in an emulate SMTP client application operation 208, determining whether dirty pages were generated during the emulation in a dirty pages generated check operation 210, and, if dirty pages were generated, saving a state of the SMTP client application including the dirty pages in a save state of SMTP client application operation 216.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Please replace the paragraph extending from page 30, line 3 to line 16 (the Abstract), with the following amended paragraph:

A method includes establishing a SMTP proxy, defining an application that forms a connection with the SMTP proxy as a SMTP client application, emulating the SMTP client application including generating at least one SMTP client application dirty page, intercepting an executable application sent from the SMTP client application with the SMTP proxy, emulating the executable application including generating at least one executable application dirty page. If a determination is made that the at least one SMTP client application dirty page is a match ~~and~~ of the at least one executable application dirty page, a determination is made that the SMTP client application is polymorphic malicious code that is attempting to send itself and protective action is taken.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888